



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Canonical Form of a Linear Homogeneous Substitution in a Galois Field.

BY LEONARD EUGENE DICKSON.

1. A simple canonical form of the general m -ary linear homogeneous substitution with integral coefficients taken modulo p , a prime, has been obtained by M. Jordan by a rather lengthy analysis.* The method may be readily generalized to apply to substitutions in an arbitrary Galois field. The present paper, however, gives a short proof by induction of the generalized theorem. That the new method is of practical value in actually reducing a given substitution to its canonical form is illustrated by the example of §3.

In §§4–7, the explicit form of all substitutions in the $GF[p^n]$ commutative with a given substitution in that field is set up. In particular, the number of such substitutions is deduced, the result being in accord with that of M. Jordan† for the case $n = 1$.

In §8 is given a simple criterion for the conjugacy of two linear homogeneous substitutions in a Galois field.

2. Consider an m -ary substitution with coefficients in the $GF[p^n]$,

$$S: \quad \xi'_i = \sum_{j=1}^m \alpha_{ij} \xi_j. \quad (i = 1, \dots, m)$$

In order that S shall multiply by a constant K the linear function

$$\eta \equiv \sum_{i=1}^m \lambda_i \xi_i,$$

*“*Traité des substitutions*,” pp. 114–126.

† *Ibid.*, p. 136.

the following conditions must be satisfied :

$$\sum_{i=1}^m \lambda_i \alpha_{ij} = K \lambda_j. \quad (j = 1, \dots, m) \quad (1)$$

Hence K must be a root of the characteristic equation

$$\Delta(K) \equiv \begin{vmatrix} \alpha_{11} - K & \alpha_{12} & \dots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} - K & \dots & \alpha_{2m} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mm} - K \end{vmatrix} = 0.$$

Corresponding to each root K , we can determine at least one set of solutions λ_i of the equations (1), and hence, at least one function η .

If $\Delta(K) = 0$ has m distinct roots $K_1, K_2, \dots, K_m$ (in general not belonging to the initial Galois field), we reach m linear functions $\eta_1, \eta_2, \dots, \eta_m$, which S multiplies by $K_1, K_2, \dots, K_m$ respectively. These functions are linearly independent. For, if constants μ_i exist such that

$$\mu_1 \eta_1 + \mu_2 \eta_2 + \dots + \mu_m \eta_m \equiv 0,$$

we have, on applying the substitutions $1, S, S^2, \dots, S^{m-1}$, the identities

$$K_1^r \mu_1 \eta_1 + K_2^r \mu_2 \eta_2 + \dots + K_m^r \mu_m \eta_m \equiv 0. \\ (r = 0, 1, \dots, m-1)$$

The determinant $|K_i^r|$ equals the product of the differences of $K_1, \dots, K_m$, and hence is not zero. Hence, must $\mu_1 = \mu_2 = \dots = \mu_m = 0$.

Introducing the linearly independent functions $\eta_1, \dots, \eta_m$ as new indices the substitution S takes the canonical form

$$S': \quad \eta'_i = K_i \eta_i. \quad (i = 1, \dots, m)$$

If we take a suitable multiple of η_1 in place of η_1 , we may suppose the reduction of S to S' to be accomplished by a transformation of indices of determinant unity.

In general, however, the roots of $\Delta(K) = 0$ are not all distinct. Let

$$\Delta(K) \equiv [F_k(K)]^a [F_l(K)]^b \dots, \quad (m = ka + lb + \dots)$$

where $F_k(K), F_l(K), \dots$ are the distinct factors of $\Delta(K)$ which belong to

and are irreducible in the $GF[p^n]$. For the roots of $F_k(K) = 0$ we employ the notation

$$K_0, K_1 \equiv K_0^{p^n}, \quad K_2 \equiv K_0^{p^{2n}}, \dots, \quad K_{k-1} \equiv K_0^{p^{n(k-1)}}.$$

Likewise, the roots of $F_l(K) = 0$ are designated

$$L_0, L_1 \equiv L_0^{p^n}, \quad L_2 \equiv L_0^{p^{2n}}, \dots, \quad L_{l-1} \equiv L_0^{p^{n(l-1)}}.$$

THEOREM.—*By a suitable transformation of indices, S can be reduced to a canonical form of the following type :*

$$\begin{aligned} \eta'_{i1} &= K_i \eta_{i1} & , & \quad \eta'_{ij} = K_i (\eta_{ij} + \eta_{ij-1}) & , \\ & & & (j = 2, \dots, a_1) & \\ \eta'_{ia_1+1} &= K_i \eta_{ia_1+1} & , & \quad \eta'_{ia_1+j} = K_i (\eta_{ia_1+j} + \eta_{ia_1+j-1}) & , \\ & & & (j = 2, \dots, a_2) & \\ \eta'_{ia_1+a_2+1} &= K_i \eta_{ia_1+a_2+1}, & \quad \eta'_{ia_1+a_2+j} &= K_i (\eta_{ia_1+a_2+j} + \eta_{ia_1+a_2+j-1}), & \\ & & & (j = 2, \dots, a_3) & \\ & \dots\dots\dots & & & \\ & & & (i = 0, 1, \dots, k-1) & \\ \zeta'_{i1} &= L_i \zeta_{i1} & , & \quad \zeta'_{ij} = L_i (\zeta_{ij} + \zeta_{ij-1}) & \\ & & & (j = 2, \dots, b_1) & \\ \zeta'_{ib_1+1} &= L_i \zeta_{ib_1+1} & , & \quad \zeta'_{ib_1+j} = L_i (\zeta_{ib_1+j} + \zeta_{ib_1+j-1}) & \\ & & & (j = 2, \dots, b_2) & \\ & \dots\dots\dots & & & \\ & & & (i = 0, 1, \dots, l-1) & \\ & \dots\dots\dots & & & \end{aligned}$$

where $a_1 + a_2 + a_3 + \dots = \alpha$, $b_1 + b_2 + \dots = \beta$, $\dots$, and where the indices have the properties :

(a). The indices η_{is} ($s = 1, \dots, \alpha$) are linear homogeneous functions of the original indices ξ_i having as coefficients polynomials in K_0 with coefficients in the $GF[p^n]$. The η_{is} are the conjugate functions derived upon replacing K_0 by K_i .

(b). The indices ζ_{is} ($s = 1, \dots, \beta$) are linear functions of the ξ_i having as coefficients polynomials in L_0 with coefficients in the $GF[p^n]$. The ζ_{is} are obtained from the ζ_{0s} upon replacing L_0 by L_i .

(c). The $k\alpha$ indices η_{is} ($i = 0, 1, \dots, k-1$; $s = 1, \dots, \alpha$) may be replaced by $k\alpha$ linear functions y_{is} of the indices ξ_i with coefficients in the $GF[p^n]$, such that S replaces each y_{is} by a linear function of the y 's alone with coefficients in the field.

(d). The $l\beta$ indices ζ_{is} may be replaced by an equal number of linear functions z_{is} belonging to the $GF[p^n]$, such that S replaces each by a linear function of the z 's alone with coefficients in the field, etc.

For the case $\alpha = \beta = \dots = 1$, we obtained above the canonical form

$$\eta'_{i1} = K_i \eta_{i1} \quad (i = 0, 1, \dots, k-1), \quad \zeta'_{i1} = L_i \zeta_{i1} \quad (i = 0, 1, \dots, l-1), \dots,$$

where η_{i1} is the same function of the ξ_j 's and K_i that η_{01} is of the ξ_j 's and K_0 , and similarly for the ζ_{i1} as functions of the L_i .

We will prove the general theorem by induction, supposing it true for every substitution belonging to the $GF[p^n]$ whose characteristic determinant has no irreducible factors other than $F_k(K)$, $F_l(K)$, $\dots$, and has these to a degree at most $\alpha - 1$, β , $\dots$ respectively. We will prove that the theorem is true for any substitution S for which these factors occur to the degree α , β , $\dots$ respectively, where $\alpha > 1$.

Corresponding to the distinct roots $K_0, K_1, \dots, K_{k-1}$ of $F_k(K) = 0$, we obtain as above a set of linearly independent conjugate functions $\lambda_0, \lambda_1, \dots, \lambda_{k-1}$ which S multiplies by $K_0, K_1, \dots, K_{k-1}$ respectively. We may introduce these in place of an equal number of the original indices, e. g., $\xi_{m-k+1}, \dots, \xi_m$. The substitution S then takes the form

$$S' \quad \begin{cases} \lambda'_i = K_i \lambda_i, & (i = 0, 1, \dots, k-1) \\ \xi'_i = \sum_{j=1}^m \beta_{ij} \xi_j + \sum_{j=0}^{k-1} \gamma_{ij} \lambda_j. & (i = 1, \dots, m-k) \end{cases}$$

The coefficients β_{ij} belong to the $GF[p^n]$. Indeed, we may set

$$\lambda_i \equiv X_0 + K_i X_1 + K_i^2 X_2 + \dots + K_i^{k-1} X_{k-1}, \\ (i = 0, 1, \dots, k-1)$$

where the X_i are linear functions of the ξ_i with coefficients in the $GF[p^n]$. Since the λ_i are linearly independent, the X_i must be independent. Since

$$|K_i^j| \equiv \prod_{r < s}^{0, \dots, k-1} (K_r - K_s) \neq 0,$$

the X_j can be expressed as linear functions of the λ_i . Taking the X_j as new indices in place of the λ_i , S' takes the form S'' , a substitution on the indices X_j

and ξ_i with coefficients in the $GF[p^n]$. But S'' replaces ξ_i by

$$\sum_{j=1}^{m-k} \beta_{ij} \xi_j + \sum_{j=0}^{k-1} \delta_{ij} X_j$$

for $i = 1, \dots, m - k$. Since these functions belong to the field for arbitrary ξ_j and X_j , the coefficients β_{ij} , δ_{ij} must belong to the field.

Since the determinant of a linear substitution is not altered by a linear transformation of indices, the determinant of S' equals the determinant of S ,

$$K_0 K_1 \dots K_{k-1} \cdot |\beta_{ij}| = D.$$

We may, therefore, consider the following substitution in the $GF[p^n]$:

$$S_1: \quad \xi'_i = \sum_{j=1}^{m-k} \beta_{ij} \xi_j \quad (i = 1, \dots, m - k)$$

of determinant $\neq 0$. Also, the characteristic determinant $\Delta(K)$ of S equals that of the transformed substitution S' , viz.:

$$\Delta(K) = \prod_{i=0}^{k-1} (K_i - K) \begin{vmatrix} \beta_{11} - K & \beta_{12} & \dots \\ \beta_{21} & \beta_{22} - K & \dots \\ \dots & \dots & \dots \end{vmatrix}.$$

Hence, the characteristic determinant of S_1 is

$$\frac{\Delta(K)}{F_k(K)} \equiv [F_k(K)^{a-1} [F_l(K)]^b \dots]$$

Hence, by hypothesis, S_1 can be reduced to a canonical form of the above type.

Applying the same transformation of indices to S' , it takes the form $\bar{S}$:

$$\begin{aligned} \lambda'_i &= K_i \lambda_i, & (i = 0, \dots, k-1) \\ \eta'_{01} &= K_0 \eta_{01} + \sum_{i=0}^{k-1} \alpha_{1i} \lambda_i, & \eta'_{0j} = K_0 (\eta_{0j} + \eta_{0j-1}) + \sum_{i=0}^{k-1} \alpha_{ji} \lambda_i, \\ & & (j = 2, \dots, a_1) \\ \eta'_{0a_1+1} &= K_0 \eta_{0a_1+1} + \sum \beta_{1i} \lambda_i, & \eta'_{0a_1+j} = K_0 (\eta_{0a_1+j} + \eta_{0a_1+j-1}) + \sum \beta_{ji} \lambda_i, \\ & & (j = 2, \dots, a_2) \\ & \dots \dots \dots \\ \zeta'_{01} &= L_0 \zeta_{01} + \sum \alpha'_{1i} \lambda_i, & \zeta'_{0j} = L_0 (\zeta_{0j} + \zeta_{0j-1}) + \sum \alpha'_{ji} \lambda_i, \\ & & (j = 2, \dots, b_1) \\ & \dots \dots \dots \end{aligned}$$

the expression for η'_{is} being derived from that for η'_{0s} by replacing K_0 by K_i ; the expression for ζ'_{is} from ζ'_{0s} upon replacing L_0 by L_i , etc.

To simplify the form of $\bar{S}$, introduce as new indices

$$Y_{0s} \equiv \eta_{0s} + \sum_{i=0}^{k-1} A_{si} \lambda_i \quad (s=1, \dots, \alpha); \quad Z_{0s} \equiv \zeta_{0s} + \sum_{i=0}^{k-1} B_{si} \lambda_i, \quad (s=1, \dots, \beta); \dots$$

and the conjugate functions $Y_{is}, Z_{is}, \dots$. Then $\bar{S}$ replaces Y_{01}, Y_{02}, Y_{03} by

$$\begin{aligned} K_0 \eta_{01} + \sum_{i=0}^{k-1} (\alpha_{1i} \lambda_i + K_i A_{1i} \lambda_i) \\ \equiv K_0 Y_{01} + \alpha_{10} \lambda_0 + \sum_{i=1}^{k-1} [\alpha_{1i} + (K_i - K_0) A_{1i}] \lambda_i, \\ K_0 (\eta_{02} + \eta_{01}) + \sum (\alpha_{2i} \lambda_i + K_i A_{2i} \lambda_i) \\ \equiv K_0 (Y_{02} + Y_{01}) + \sum_{i=0}^{k-1} [\alpha_{2i} - K_0 A_{1i} + (K_i - K_0) A_{2i}] \lambda_i, \\ K_0 (\eta_{03} + \eta_{02}) + \sum (\alpha_{3i} \lambda_i + K_i A_{3i} \lambda_i) \\ \equiv K_0 (Y_{03} + Y_{02}) + \sum_{i=0}^{k-1} [\alpha_{3i} - K_0 A_{2i} + (K_i - K_0) A_{3i}] \lambda_i. \end{aligned}$$

Each term of the sums on the right may be made zero by choice of the A_{ji} , viz., the terms of the first sum by choice of $A_{11}, \dots, A_{1, k-1}$; those of the second sum by choice of $A_{10}, A_{21}, \dots, A_{2, k-1}$; those of the third sum by choice of $A_{20}, A_{31}, \dots, A_{3, k-1}$. A like result holds for all of the Y_{0s} ($s=1, \dots, \alpha$).

$\bar{S}$ replaces $Z_{01}, Z_{02}, \dots$ by respectively

$$\begin{aligned} L_0 Z_{01} + \sum_{i=0}^{k-1} [\alpha'_{1i} + (K_i - L_0) B_{1i}] \lambda_i, \\ L_0 (Z_{02} + Z_{01}) + \sum_{i=0}^{k-1} [\alpha'_{2i} - L_0 B_{1i} + (K_i - L_0) B_{2i}] \lambda_i, \dots \end{aligned}$$

Since $K_i - L_0 \neq 0$, the coefficients of λ_i may be made to vanish by choice of the B_{si} . Hence, $\bar{S}$ takes the form S_2 :

$$\lambda'_i = K_i \lambda_i,$$

$$\begin{aligned}
Y'_{i1} &= K_i Y_{i1} + \phi(K_i) \lambda_i, & Y'_{ij} &= K_i (Y_{ij} + Y_{ij-1}), \\
&& (j=2, \dots, a_1) \\
Y'_{ia_1+1} &= K_i Y_{ia_1+1} + \psi(K_i) \lambda_i, & Y'_{ia_1+j} &= K_i (Y_{ia_1+j} + Y_{ia_1+j-1}), \\
&& (j=2, \dots, a_2) \\
&\dots\dots\dots \\
&& (i=0, 1, \dots, k-1) \\
Z'_{i1} &= L_i Z_{i1}, & Z'_{ij} &= L_i (Z_{ij} + Z_{ij-1}), \\
&& (j=2, \dots, b_1) \\
Z'_{ib_1+1} &= L_i Z_{ib_1+1}, & Z'_{ib_1+j} &= L_i (Z_{ib_1+j} + Z_{ib_1+j-1}). \\
&& (j=2, \dots, b_2) \\
&\dots\dots\dots \\
&& (i=0, 1, \dots, l-1)
\end{aligned}$$

If the constants $\phi(K_i)$, $\psi(K_i)$, $\chi(K_i)$, ... are all zero, no further reduction is necessary. If any two are not zero, as ϕ and ψ , suppose for definiteness that $a_1 \leq a_2$, and introduce in place of $Y_{i1}, \dots, Y_{ia_1}$ the new indices

$$\overline{Y}_{ij} \equiv Y_{ij} - \frac{\phi}{\psi} Y_{ia_1+j}. \quad (i=1, \dots, a_1).$$

The substitution S_2 replaces $\overline{Y}_{i1}, \overline{Y}_{ij} (j=2, \dots, a_1)$ by respectively

$$K_i \overline{Y}_{i1}, \quad K_i (\overline{Y}_{ij} + \overline{Y}_{ij-1}). \quad (j=2, \dots, a_1)$$

Hence, the introduction of the $\overline{Y}_{ij}$ has the effect of setting $\phi=0$ in S_2 . Proceeding similarly, we can suppose that $\phi, \psi, \chi, \dots$ are all zero but one, say $\psi \neq 0$. In the latter case, we set

$$\psi(K_i) \cdot \lambda_i \equiv K_i y_{ia_1}$$

and find for S_2 the canonical form

$$\begin{aligned}
Y'_{i1} &= K_i Y_{i1}, & Y'_{ij} &= K_i (Y_{ij} + Y_{ij-1}), & (j=2, \dots, a_1) \\
y'_{ia_1} &= K_i y_{ia_1}, & Y'_{ia_1+1} &= K_i (Y_{ia_1+1} + y_{ia_1}), \\
Y'_{ia_1+a_2+1} &= K_i Y_{ia_1+a_2+1}, & Y'_{ia_1+j} &= K_i (Y_{ia_1+j} + Y_{ia_1+j-1}), & (j=2, \dots, a_2) \\
&& Y'_{ia_1+a_2+j} &= K_i (Y_{ia_1+a_2+j} + Y_{ia_1+a_2+j-1}), & (j=2, \dots, a_3) \\
&\dots\dots\dots \\
Z'_{i1} &= L_i Z_{i1}, & Z'_{ij} &= L_i (Z_{ij} + Z_{ij-1}), & (j=2, \dots, b_1) \\
&\dots\dots\dots
\end{aligned}$$

In every case we reach a canonical form of the type given in the theorem,

for which the indices Y_{is} have the properties (a). But the indices Z_{ij} are linear functions of the ξ_i with coefficients which certainly involve L_i and apparently* also K_i . If the K_i be involved, we proceed as follows: From the canonical form actually reached, $S = YS_1$, where Y is the partial substitution on the indices Y_{ij} not altering the indices Z_{ij} , etc., while S_1 does not involve the indices Y_{ij} , but affects the Z_{ij} , etc. Setting

$$Y_{is} \equiv y_s + y'_s K_i + y''_s K_i^2 + y_s^{(k-1)} K_i^{k-1}, \\ (s = 1, \dots, \alpha; i = 0, \dots, k-1)$$

where the y 's are linear functions of the ξ_i with coefficients in the $GF[p^n]$, we can evidently introduce the y 's as new indices in place of the Y_{is} , so that Y takes the form of a substitution belonging to the $GF[p^n]$ and affecting only $k\alpha$ indices. Likewise, by introducing in place of the Z_{ij} , etc., an equal number of linear functions z_{ij} , etc., belonging to the $GF[p^n]$, it is possible to give to S_1 the form of a substitution in the field and affecting only $m - k\alpha$ indices. Its characteristic determinant is $[F_l(K)]^\beta \dots$. Hence, by the hypothesis made for the induction, S_1 can be reduced by a linear transformation T to a canonical form

$$\zeta'_{i1} = L_i \zeta_{i1}, \quad \zeta'_{ij} = L_i (\zeta_{i1} + \zeta_{ij-1}), \quad (j = 2, \dots, b_1) \\ \dots\dots\dots$$

where the ζ_{ij} are linear functions of the ζ_i with coefficients involving the imaginary L_i only. As the transformation T does not alter the indices which Y affects, we obtain the desired canonical form.

3. Consider as an example the substitution in the $GF[p^n]$, p^n of the form $4l - 1$,

$$S: \quad \xi'_1 = -2\xi_2 - \xi_4, \quad \xi'_2 = \xi_1, \quad \xi'_3 = \xi_2, \quad \xi'_4 = \xi_3,$$

having the characteristic determinant

$$\Delta(K) \equiv (K^2 + 1)^2,$$

where $K^2 + 1$ is irreducible in the field. A root of $i^2 = -1$ belongs to the $GF[p^{2n}]$ but not to the $GF[p^n]$. The functions which S multiplies by i and

By the considerations in the text, we may dispense with the difficult proof, analogous to that of Jordan, "Traité," pp. 121-122, that the Z_i do not involve K , but the single imaginary L_i .

while, for $i = 0, 1, \dots, l-1$, Z_i denotes the substitution on $b_1 + b_2 + \dots + b_{s+1} \equiv \beta$ indices:

$$\begin{aligned} \zeta'_{i1} &= L_i \zeta_{i1}, & \zeta'_{ij} &= L_i (\zeta_{ij} + \zeta_{i,j-1}), & (j = 2, \dots, b_1) \\ \zeta'_{i b_1+1} &= L_i \zeta_{i b_1+1}, & \zeta'_{i b_1+j} &= L_i (\zeta_{i b_1+j} + \zeta_{i b_1+j-1}), & (j = 2, \dots, b_2) \\ & \dots\dots\dots \end{aligned}$$

where in each case are written only those indices which the substitution alters.

Let B be a second m -ary linear homogeneous substitution in the $GF[p^n]$, and suppose it to be expressed in terms of the above indices $\eta_{is}, \zeta_{is}, \dots$, by means of which the given substitution S is reduced to the above canonical form.

THEOREM.—*In order that B shall be commutative with S , it is necessary and sufficient that the following two conditions be satisfied:*

(1). *B shall break up into the product*

$$B = y_0 y_1 \dots y_{k-1} z_0 z_1 \dots z_{l-1} \dots,$$

where y_0 is a substitution of determinant $\neq 0$ altering only the indices $\eta_{01}, \dots, \eta_{0\alpha}$:

$$\eta'_{0s} = \sum_{j=1}^{\alpha} \beta_{sj}(K_0) \eta_{0j}, \quad (s = 1, \dots, \alpha)$$

the coefficients $\beta_{sj}(K_0)$ being polynomials in K_0 with coefficients in the $GF[p^n]$, and for $i = 0, 1, \dots, k-1$, y_i denotes the conjugate substitution

$$\eta'_{is} = \sum_{j=1}^{\alpha} \beta_{sj}(K_i) \eta_{ij}, \quad (s = 1, \dots, \alpha)$$

while, similarly, z_i (for $i = 0, 1, \dots, l-1$) denotes the substitution of determinant $\neq 0$ altering only $\zeta_{i1}, \dots, \zeta_{i\beta}$, viz.,

$$\zeta'_{is} = \sum_{j=1}^{\beta} \gamma_{sj}(L_i) \zeta_{ij}. \quad (s = 1, \dots, \beta)$$

(2). Y_0 and y_0 shall be commutative, Z_0 and z_0 shall be commutative, etc.

The method of proof is sufficiently illustrated by the developments of Jordan ("Traité," pp. 128-132) upon a particular example.

5. As an important example, suppose that S has the canonical form

$$\begin{aligned} \eta'_i &= K_i \eta_i. & (i = 0, 1, \dots, k-1) \\ \zeta'_i &= L_i \zeta_i, & (i = 0, 1, \dots, l-1), \dots, \\ \xi'_i &= R_i \xi_i. & (i = 0, 1, \dots, r-1) \end{aligned}$$

Then B has the form

$$\begin{aligned}\eta'_i &= \kappa(K_i) \eta_i, & (i = 0, 1, \dots, k-1) \\ \zeta'_i &= \lambda(L_i) \zeta_i, & (i = 0, 1, \dots, l-1), \dots, \\ \xi'_i &= \rho(R_i) \xi_i. & (i = 0, 1, \dots, r-1)\end{aligned}$$

If $K, L, \dots, R$ be primitive roots of the Galois fields of orders $p^{nk}, p^{nl}, \dots, p^{nr}$ respectively, we may set

$$\kappa(K_0) = K^a, \quad \lambda(L_0) = L^b, \dots, \quad \rho(R_0) = R^c.$$

Then B takes the form

$$\begin{aligned}\eta'_i &= K^{ap^{ni}} \eta_i, & (i = 0, \dots, k-1) \\ \zeta'_i &= L^{bp^{ni}} \zeta_i, & (i = 0, \dots, l-1), \dots, \\ \xi'_i &= R^{cp^{ni}} \xi_i. & (i = 0, \dots, r-1)\end{aligned}$$

6. While investigating the conditions under which Y_0 is commutative with y_0 , we write Y_0 in the form (where we set $\eta_j \equiv \eta_{0j}$):

$$Y_0 \quad \begin{cases} \eta'_j = K_0 \eta_j, & j = 1, a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1 \\ \eta'_j = K_0(\eta_j + \eta_{j-1}). & j = 2, \dots, \alpha; j \neq a_1 + 1, \dots, a_1 + \dots + a_r + 1 \end{cases}$$

The most general form possible for y_0 is

$$y_0: \quad \eta'_i = \sum_{j=1}^{\alpha} \alpha_{ij} \eta_j. \quad (i = 1, \dots, \alpha)$$

Equating the expressions by which $y_0 Y_0$ and $Y_0 y_0$ replace η_i , where $i = 1, a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1$, in succession, we find the conditions

$$\alpha_{ij} = 0. \quad \left(\begin{matrix} j = 2, \dots, \alpha; j \neq a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1 \\ i = 1, a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1. \end{matrix} \right) \quad (2)$$

Equating the expressions by which they replace η_i , where, in succession, $i = 1, \dots, \alpha; i \neq 1, a_1 + 1, \dots, a_1 + \dots + a_r + 1$, we obtain the condition

$$\sum_{\substack{j=2, \dots, \alpha \\ j \neq a_1 + 1, \dots, a_1 + \dots + a_r + 1}} \alpha_{ij} \eta_{j-1} = \sum_{j=1}^{\alpha} \alpha_{i-1, j} \eta_j \equiv \sum_{j=2}^{a+1} \alpha_{i-1, j-1} \eta_{j-1}.$$

Hence, for $i = 2, \dots, \alpha; i \neq a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + a_2 + \dots + a_r + 1$,
 $\alpha_{i-1j-1} = 0, \quad (j = a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1, \alpha + 1) \quad (3)$
 $\alpha_{i-1j-1} = \alpha_{ij}, \quad (j = 2, \dots, \alpha; j \neq a_1 + 1, a_1 + a_2 + 1, \dots, a_1 + \dots + a_r + 1) \quad (4)$

By way of example, suppose $r = 2$ and that $a_1 = a_2 = 4, a_3 = 2$. Then by (2), (3), (4),

$$\begin{aligned} \alpha_{1j} = \alpha_{5j} = \alpha_{9j} &= 0, & (j = 2, 3, 4, 6, 7, 8, 10) \\ \alpha_{j4} = \alpha_{j8} = \alpha_{j10} &= 0, & (j = 1, 2, 3, 5, 6, 7, 9) \\ \alpha_{ij} &= \alpha_{i-1j-1}. & (i, j = 2, 3, 4, 6, 7, 8, 10) \end{aligned}$$

Hence y_0 takes the form

	η_1	η_2	η_3	η_4	η_5	η_6	η_7	η_8	η_9	η_{10}
$\eta'_1 =$	α_{11}	0	0	0	α_{15}	0	0	0	0	0
$\eta'_2 =$	α_{21}	α_{11}	0	0	α_{25}	α_{15}	0	0	0	0
$\eta'_3 =$	α_{31}	α_{21}	α_{11}	0	α_{35}	α_{25}	α_{15}	0	α_{39}	0
$\eta'_4 =$	α_{41}	α_{31}	α_{21}	α_{11}	α_{45}	α_{35}	α_{25}	α_{15}	α_{49}	α_{39}
$\eta'_5 =$	α_{51}	0	0	0	α_{55}	0	0	0	0	0
$\eta'_6 =$	α_{61}	α_{51}	0	0	α_{65}	α_{55}	0	0	0	0
$\eta'_7 =$	α_{71}	α_{61}	α_{51}	0	α_{75}	α_{65}	α_{55}	0	α_{79}	0
$\eta'_8 =$	α_{81}	α_{71}	α_{61}	α_{51}	α_{85}	α_{75}	α_{65}	α_{55}	α_{89}	α_{79}
$\eta'_9 =$	α_{91}	0	0	0	α_{95}	0	0	0	α_{99}	0
$\eta'_{10} =$	α_{101}	α_{91}	0	0	α_{105}	α_{95}	0	0	α_{109}	α_{99}

By simple interchange of rows and columns, we see that the determinant of the above substitution on ten indices equals

$$\alpha_{99}^2 \begin{vmatrix} \alpha_{11} & \alpha_{15} \\ \alpha_{51} & \alpha_{55} \end{vmatrix}^4.$$

7. For the general case, the matrix of y_0 may be considered to be made up of $(r+1)^2$ rectangles, the general one of which R_{ij} includes $a_i a_j$ coefficients α_{rs} . If $a_i \leq a_j$, this rectangle includes a square array S_i of coefficients, a_i to a side. The coefficients in its diagonal are all equal, likewise those in any parallel to the diagonal. All coefficients of the rectangle R_{ij} which lie above or to the right of the diagonal of the square S_i are zeros. The total number of distinct coefficients

$\neq 0$ is, therefore, (supposing $a_1 \geq a_2 \geq a_3 \geq \dots$),

$$\begin{aligned} & (a_1 + a_2 + a_3 + \dots + a_{r+1}) + (a_2 + a_2 + a_3 + \dots + a_{r+1}) \\ & + (a_3 + a_3 + a_3 + \dots + a_{r+1}) + \dots + (a_{r+1} + a_{r+1} + a_{r+1} + \dots + a_{r+1}) \\ & \equiv a_1 + 3a_2 + 5a_3 + 7a_4 + \dots + (2k-1)a_k + \dots + (2r+1)a_{r+1}, \quad (5), \end{aligned}$$

the quantities in the j^{th} parenthesis being the number of distinct coefficients $\neq 0$ in the j^{th} row of rectangles.

To fix the ideas, let

$$a_1 = a_2 = \dots = a_\lambda \equiv a, \quad a_{\lambda+1} = a_{\lambda+2} = \dots = a_{\lambda+\mu} \equiv b, \quad a_{\lambda+\mu+1} = \dots = a_{\lambda+\mu+\rho} \equiv c,$$

$$\text{where} \quad a > b > c, \quad \lambda + \mu + \rho \equiv r + 1.$$

We proceed to prove that the determinant of y_0 equals

$$|y_0| = D_\lambda D_\mu D_\rho,$$

where

$$\begin{aligned} D_\lambda & \equiv \begin{vmatrix} \alpha_{11} & \alpha_{1 \ a+1} & \alpha_{1 \ 2a+1} & \dots & \alpha_{1 \ \lambda a - a + 1} \\ \alpha_{a+1 \ 1} & \alpha_{a+1 \ a+1} & \alpha_{a+1 \ 2a+1} & \dots & \alpha_{a+1 \ \lambda a - a + 1} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{\lambda a - a + 1 \ 1} & \alpha_{\lambda a - a + 1 \ a+1} & \alpha_{\lambda a - a + 1 \ 2a+1} & \dots & \alpha_{\lambda a - a + 1 \ \lambda a - a + 1} \end{vmatrix}. \\ D_\mu & \equiv \begin{vmatrix} \alpha_{\lambda a + 1 \ \lambda a + 1} & \alpha_{\lambda a + 1 \ \lambda a + b + 1} & \dots & \alpha_{\lambda a + 1 \ \lambda a + \mu b - b + 1} \\ \dots & \dots & \dots & \dots \\ \alpha_{\lambda a + \mu b - b + 1 \ \lambda a + 1} & \alpha_{\lambda a + \mu b - b + 1 \ \lambda a + b + 1} & \dots & \alpha_{\lambda a + \mu b - b + 1 \ \lambda a + \mu b - b + 1} \end{vmatrix}. \\ D_\rho & \equiv \begin{vmatrix} \alpha_{\lambda a + \mu b + 1 \ \lambda a + \mu b + 1} & \dots & \alpha_{\lambda a + \mu b + 1 \ \lambda a + \mu b + \rho c - c + 1} \\ \dots & \dots & \dots \\ \alpha_{\lambda a + \mu b + \rho c - c + 1 \ \lambda a + \mu b + 1} & \dots & \alpha_{\lambda a + \mu b + \rho c - c + 1 \ \lambda a + \mu b + \rho c - c + 1} \end{vmatrix}. \end{aligned}$$

Indeed, the coefficients of $\eta_1, \eta_{a+1}, \eta_{2a+1}, \dots, \eta_{\lambda a+1}, \eta_{\lambda a+b+1}, \dots, \eta_{\lambda a+\mu b+\rho c-c+1}$ in $\eta'_1, \eta'_{a+1}, \eta'_{2a+1}, \dots$, form a matrix of the form

$$(D) = \left(\begin{array}{c|c|c} (D_\lambda) & \text{zeros} & \text{zeros} \\ \hline & (D_\mu) & \text{zeros} \\ \hline & & (D_\rho) \end{array} \right)$$

of determinant $D = D_\lambda D_\mu D_\rho$. All the coefficients of $\eta'_1, \eta'_{a+1}, \dots, \eta'_{\lambda a+\mu b+\rho c-c+1}$ are zeros except those in the matrix (D) . Hence,

$$|y_0| = D_\lambda D_\mu D_\rho \cdot D_1,$$

D_1 being the determinant of the matrix (D_1) obtained from the matrix for y_0 upon deleting the $1^{\text{st}}, a+1^{\text{st}}, 2a+1^{\text{st}}, \dots, \lambda a+\mu b+\rho c-c+1^{\text{st}}$ rows and columns. Selecting from (D_1) the coefficients of $\eta_2, \eta_{a+2}, \eta_{2a+2}, \dots$ in $\eta'_2, \eta'_{a+2}, \dots$, we obtain the matrix (D) . Deleting the corresponding rows and columns from (D_1) , we obtain a matrix (D_2) , whose determinant D_2 is given by

$$D_1 = DD_2.$$

After c such operations, we reach a matrix (D_c) whose determinant D_c is given by the equation

$$|y_0| = D^c D_c.$$

In the matrix (D_c) , the coefficients of $\eta_{c+1}, \eta_{a+c+1}, \dots, \eta_{\lambda a+c+1}, \eta_{\lambda a+b+c+1}, \dots, \eta_{\lambda a+\mu b-b+c+1}$ in $\eta'_{c+1}, \eta'_{a+c+1}, \dots$, form a matrix

$$(E) \equiv \left(\begin{array}{c|c} (D_\lambda) & \text{zeros} \\ \hline & (D_\mu) \end{array} \right)$$

of determinant $E = D_\lambda D_\mu$. In (D_c) all the coefficients of $\eta'_{c+1}, \eta'_{a+c+1}, \dots$ are zero except those in (E) . Hence,

$$D_c = E \cdot E_1,$$

where E_1 is the determinant of the matrix (E_1) obtained by deleting the $1^{\text{st}}, a+1^{\text{st}}, 2a+1^{\text{st}}, \dots, \lambda a+\mu b-b+1^{\text{st}}$ rows and columns from (D_c) . Selecting the coefficients of $\eta_{c+2}, \eta_{a+c+2}, \dots$ in $\eta'_{c+2}, \dots$ from the matrix (E_1) , we obtain the matrix (E) . Deleting from (E_1) the $2^{\text{nd}}, a+2^{\text{nd}}, \dots$ rows and columns, we obtain a matrix (E_2) , whose determinant E_2 is given by the equation $E_1 = EE_2$. After $b-c$ such steps, we reach a matrix (E_{b-c}) whose determinant is given by

$$D_c = E^{b-c} E_{b-c}.$$

In the matrix (E_{b-c}) , the coefficients of $\eta_{b+i}, \eta_{a+b+i}, \dots, \eta_{\lambda a-a+b+i}$ in $\eta'_{b+i}, \eta'_{a+b+i}, \dots, \eta'_{\lambda a-a+b+i}$ (for each value of $i = 1, 2, \dots, a-b$), form the matrix (D_λ) . Hence,

$$E_{b-c} = D_\lambda^{a-b}.$$

Hence, $|y_0| = (D_\lambda D_\mu D_\rho)^c (D_\lambda D_\mu)^{b-c} D_\lambda^{a-b} \equiv D_\lambda^a D_\mu^b D_\rho^c$.

There are $\lambda^2 + \mu^2 + \rho^2$ distinct coefficients entering the determinants D_λ, D_μ, D_ρ . These are subject to the conditions that the determinants shall not vanish.

By (5), the total number of non-vanishing coefficients of y_0 is seen to be

$$a\lambda^2 + b(\mu^2 + 2\lambda\mu) + c(\rho^2 + 2\lambda\rho + 2\mu\rho).$$

The number of absolutely arbitrary coefficients in y_0 is, therefore,

$$\lambda^2(a-1) + \mu^2(b-1) + \rho^2(c-1) + 2b\lambda\mu + 2c\lambda\rho + 2c\mu\rho.$$

To formulate our theorem for the most general case, let

$$a_1 = a_2 = \dots = a_{\lambda_1} \equiv A_1; \quad a_{\lambda_1+1} = \dots = a_{\lambda_1+\lambda_2} \equiv A_2; \dots; \\ a_{\lambda_1+\lambda_2+\dots+\lambda_{s-1}+1} = \dots = a_{\lambda_1+\lambda_2+\dots+\lambda_s} \equiv A_s,$$

where $A_1 > A_2 > \dots > A_s; \quad \lambda_1 + \lambda_2 + \dots + \lambda_s = r + 1.$

The determinant of y_0 equals

$$D_{\lambda_1}^{A_1} D_{\lambda_2}^{A_2} \dots D_{\lambda_s}^{A_s}.$$

The coefficients α_{ij} being functions of K_0 , a root of an irreducible equation of degree k belonging to the $GF[p^n]$, the number of sets of values for the λ_i^2 coefficients entering D_{λ} for which this determinant $\neq 0$ is*

$$N_i \equiv (p^{nk\lambda_i} - 1)(p^{nk\lambda_i} - p^{nk}) \dots (p^{nk\lambda_i} - p^{nk(\lambda_i-1)}).$$

Hence, there are $N_1 N_2 \dots N_s$ sets of values for the $\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \dots + \lambda_s^2$ distinct coefficients entering these determinants. But by (5), the number of distinct coefficients in y_0 is

$$A_1 \lambda_1^2 + A_2 \lambda_2 (\lambda_2 + 2\lambda_1) + A_3 \lambda_3 (\lambda_3 + 2\lambda_2 + 2\lambda_1) + \dots \\ + A_s \lambda_s (\lambda_s + 2\lambda_{s-1} + \dots + 2\lambda_1).$$

There remain the following number of wholly arbitrary coefficients:

$$A \equiv \sum_{i=1}^s \lambda_i^2 (A_i - 1) + 2A_2 \lambda_2 \lambda_1 + 2A_3 \lambda_3 (\lambda_2 + \lambda_1) + \dots \\ + 2A_s \lambda_s (\lambda_{s-1} + \dots + \lambda_2 + \lambda_1).$$

Each of these has p^{nk} distinct values. The total number of substitutions y_0 commutative with Y_0 is, therefore,

$$N_1 N_2 \dots N_s \cdot p^{nkA}. \quad (6)$$

For the above example, viz., $a_1 = a_2 = a_4, \quad a_3 = 2$, this number is

$$p^{21nk} (p^{2nk} - 1)(p^{2nk} - p^{nk})(p^{nk} - 1),$$

as is evident by inspecting the form of y_0 .

* Jordan, "Traité," p. 135; Dickson, *Annals of Mathematics*, 1897, p. 164.

8. THEOREM.—Two real linear homogeneous substitutions S and T on the indices $\xi_1, \dots, \xi_m$ have the same canonical form C if, and only if, T is the transformed of S by a real linear homogeneous substitution W on the same indices.*

If $T = W^{-1}SW$, S can be reduced to T by the introduction of new indices defined by the real transformation W . Hence, S and T have the same canonical form.

Suppose, inversely, that two real substitutions S and T on the indices ξ_i can be reduced to the same canonical form by transformations $[S]$ and $[T]$ respectively. Let $[T]$ denote the transformation from the indices $\xi_1, \dots, \xi_m$ to the indices $\eta_{is}, \zeta_{is}, \dots$, where

$$\begin{aligned}\eta_{is} &\equiv Y_s + Y'_s K_i + Y''_s K_i^2 + \dots + Y_s^{(k-1)} K_i^{k-1}, \\ &\quad (s = 1, \dots, \alpha; i = 0, 1, \dots, k-1) \\ \zeta_{is} &\equiv Z_s + Z'_s L_i + Z''_s L_i^2 + \dots + Z_s^{(l-1)} L_i^{l-1}, \\ &\quad (s = 1, \dots, \beta; i = 0, 1, \dots, l-1) \\ &\dots\dots\dots\end{aligned}$$

where $Y_s, Y'_s, \dots, Z_s, \dots$ are $k\alpha$ real linear functions of the ξ_i , which are linearly independent. Denote by τ the transformation of indices from $\eta_{is}, \zeta_{is}, \dots$ to $Y_s, Y'_s, \dots, Z_s, \dots$. By hypothesis, $[T]$ transforms T into the canonical form C . Let τ transform C into C_τ . Then $[T]\tau$ is a real substitution which transforms T into C_τ , a real substitution on real indices.

Similarly, let $[S]$ denote the transformation from the indices $\xi_1, \dots, \xi_m$ to the indices $\overline{\eta}_{is}, \overline{\zeta}_{is}, \dots$, where

$$\overline{\eta}_{is} \equiv \overline{Y}_s + \overline{Y}'_s K_i + \dots, \quad \overline{\zeta}_{is} \equiv \overline{Z}_s + \overline{Z}'_s L_i + \dots, \quad \dots$$

Denote by σ the transformation of indices from $\overline{\eta}_{is}, \overline{\zeta}_{is}, \dots$ to $\overline{Y}_s, \dots, \overline{Z}_s, \dots$. By hypothesis, $[S]$ transforms S into the canonical form $\overline{C}$, which is the same substitution on the indices $\overline{\eta}_{is}, \overline{\zeta}_{is}, \dots$ that C is on the indices $\eta_{is}, \zeta_{is}, \dots$. Let σ transform $\overline{C}$ into $\overline{C}_\sigma$. Hence, if R be the real substitution transforming $Y_s, \dots, Z_s, \dots$ into $\overline{Y}_s, \dots, \overline{Z}_s, \dots$ respectively,

$$\overline{C}_\sigma = R^{-1} C_\tau R.$$

It follows that the product

$$[T] \tau R ([S] \sigma)^{-1}$$

is a real substitution on the indices ξ_i which transforms T into S .

*In §§8-9, we speak of a function or substitution as *real* if its coefficients belong to the $GF[p^n]$.

9. As a corollary to the theorem of §8, we have the theorem:

In order that a real substitution S whose canonical form has the multipliers $M_1, M_2, \dots, M_m$ shall be transformed by a real substitution of a real substitution whose canonical form has the multipliers $\Theta M_1, \Theta M_2, \dots, \Theta M_m$, it is necessary that the two sets of multipliers be identical apart from their order. Hence, $\Theta^m = 1$.

If $m = 3$, $\Theta \neq 1$, and if S have determinant unity, it is necessary that M_1, M_2, M_3 be in some order equal to $1, \Theta, \Theta^2$.

Indeed, since $\Theta M_1 \neq M_1$, we may set $\Theta M_1 = M_2$, properly choosing the notation for M_2 and M_3 . Then $\Theta M_2 \neq M_1$; for if so, $\Theta^2 = 1$, and hence $\Theta = 1$. Hence, $\Theta M_2 = M_3$, $\Theta M_3 = M_1$. Hence, the multipliers are

$$M_1, M_2 = \Theta M_1, M_3 = \Theta^2 M_1. \quad (\Theta^3 = 1).$$

The determinant of S being unity,

$$M_1 M_2 M_3 = 1 = \Theta^3 M_1^3.$$

Hence, $M_1^3 = 1$, so that M_3 is a power of Θ . The theorem is, therefore, proven.

In like manner, we may prove that for $m = 4$, $\Theta \neq 1$ and S of determinant unity, it is necessary that the multipliers M_1, M_2, M_3, M_4 be in some order either

$$M_1, \Theta M_1, \frac{1}{M_1}, \frac{\Theta}{M_1}, \quad (\Theta^2 = 1, M_1 \text{ arbitrary})$$

or

$$M_1, \Theta M_1, \Theta^2 M_1, \Theta^3 M_1, \quad (\Theta^2 = -1, M_1^4 = \Theta^2 = -1),$$

there being a single distinct set of multipliers in the latter case.

These results find constant application in the problem of the determination of the subgroups of the simple groups of all linear fractional substitutions of determinant unity in two or three non-homogeneous variables with coefficients in an arbitrary Galois field.